

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-342270

(43)Date of publication of application : 29.11.2002

(51)Int.Cl.

G06F 15/00

G06F 12/00

G06F 12/14

G06F 13/00

(21)Application number : 2001-145886

(71)Applicant : JAPAN TELECOM HOLDINGS CO LTD

(22)Date of filing : 16.05.2001

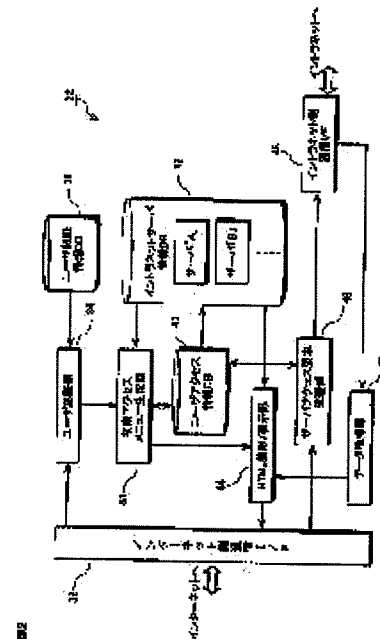
(72)Inventor : KOBAYASHI JUNYA

## (54) REMOTE ACCESS CONTROL METHOD AND REMOTE ACCESS CONTROL PROGRAM

(57)Abstract:

PROBLEM TO BE SOLVED: To perform an access from the outside to a server on an intranet without having to conduct complicated input on the part of a user.

SOLUTION: A remote access control server 22 is provided with a user authenticating part 34 for receiving log-in and user ID and a password from a portable terminal 14, and for authenticating the user, an initial access menu generating part 38 for generating a list related with a server which can be accessed by the authenticated user, and for transmitting the list to a portable terminal 14, an access information receiving part 46 for specifying the server to be accessed on the intranet 24, based on an item selected from the list, and for acquiring authentication information specific to the user related with the server, and for transmitting the authentication information through the intranet 24, and for realizing the transmission of contents, in response to the user authentication and the selected item, and an information acquiring part 50 for receiving the contents, in response to the item from the server. Then, the acquired contents are transmitted to the portable terminal 14.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号  
特開2002-342270  
(P2002-342270A)

(43) 公開日 平成14年11月29日 (2002.11.29)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	ページ* (参考)
G 0 6 F 15/00	3 1 0	G 0 6 F 15/00	3 1 0 D 5 B 0 1 7
	3 3 0		3 3 0 B 5 B 0 8 2
12/00	5 3 7	12/00	5 3 7 D 5 B 0 8 5
	5 4 6		5 4 6 A
12/14	3 2 0	12/14	3 2 0 C

審査請求 未請求 請求項の数10 O L (全 11 頁) 最終頁に続く

(21) 出願番号 特願2001-145886(P2001-145886)

(22) 出願日 平成13年5月16日 (2001.5.16)

(71) 出願人 000229265

日本テレコムホールディングス株式会社  
東京都中央区八丁堀四丁目7番1号

(72) 発明者 小林 純也

東京都中央区八丁堀四丁目7番1号 日本  
テレコム株式会社内

(74) 代理人 100103632

弁理士 窪田 英一郎 (外1名)

Fターム(参考) 5B017 AA07 BA05 CA16

5B082 GA11 IIA08

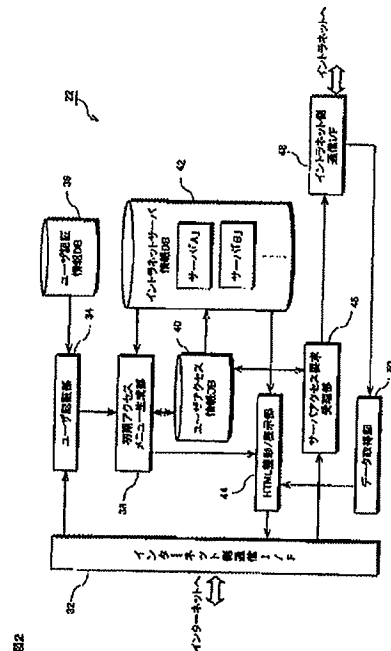
5B085 AED1 AE23 BC07

(54) 【発明の名称】 リモートアクセス制御方法、リモートアクセス制御プログラム

(57) 【要約】

【課題】 ユーザによる煩雑な入力なしに、イントラネット上のサーバに外部からアクセスする。

【解決手段】 リモートアクセス制御サーバ22は、携帯端末14からログインおよびユーザIDおよびパスワードを受理して、ユーザを認証するユーザ認証部34と、認証されたユーザがアクセス可能なサーバに関するリストを生成して、当該リストを、携帯端末14に伝達する初期アクセスメニュー生成部38と、携帯端末14からの、リストから選択された項目に基づき、イントラネット24上のアクセスすべきサーバを特定して、サーバに関するユーザ固有の認証情報を取得して、イントラネット24を介して認証情報を伝達して、ユーザ認証および選択された項目に応答したコンテンツの伝達を求めるアクセス情報受理部46と、サーバから、項目に応答したコンテンツを受理する情報取得部50とを備え、取得したコンテンツが携帯端末14に伝達されるようになっている。



## 【特許請求の範囲】

【請求項1】 所定のネットワークに接続された複数のサーバに、当該ネットワークの外部の端末からアクセスするためのリモートアクセス制御方法であって、前記所定のネットワークに接続されたリモートアクセス制御サーバにおいて、前記端末によるアクセスをなすユーザによる前記ネットワークへのログインのための認証情報を登録するステップと、

前記ユーザがアクセス可能な前記ネットワーク上のサーバのそれぞれに関する、当該ユーザの固有の認証情報を登録するステップと、

前記端末からの、前記ログインのための認証情報の受理に応答して、ユーザを認証するステップと、

認証されたユーザがアクセス可能なサーバに関するリストを生成して、当該リストを、前記端末に伝達するステップと、

前記端末からの、リストから選択された項目に基づき、前記ネットワーク上のアクセスすべきサーバを特定するステップと、

前記サーバに関する前記ユーザの固有の認証情報を取得して、当該サーバに対して、認証情報を伝達して、ユーザ認証および選択された項目に応答したコンテンツの伝達を求めるステップと、

前記サーバから、前記項目に応答したコンテンツを受理するステップと、

受理したコンテンツを、前記端末に伝達するステップとを備えたことを特徴とするリモートアクセス制御方法。

【請求項2】 前記ユーザの固有の認証情報を登録するステップが、前記認証の種類を含み、前記サーバに関する前記ユーザ固有の認証情報を、前記サーバに対して伝達するステップが、前記認証の種類にしたがった情報の伝達を行うことを特徴とする請求項1に記載のリモートアクセス制御方法。

【請求項3】 前記サーバに関する前記ユーザ固有の認証情報を、前記サーバに対して伝達するステップが、ベーシック認証におけるユーザIDおよびパスワードを伝達するステップを含むことを特徴とする請求項1または2に記載のリモートアクセス制御方法。

【請求項4】 さらに、前記受理したコンテンツにリンクが含まれる場合に、前記リンクを、前記リモートアクセスサーバを介した形態のものに変換するステップを備えたことを特徴とする請求項1ないし3の何れか一項に記載のリモートアクセス制御方法。

【請求項5】 さらに、前記コンテンツにおけるフォントサイズの変更、テーブルの列幅の調整を含むコンテンツ表示形態の調整、および／または、不要なタグの消去を含む、コンテンツを整形するステップを備えたことを特徴とする請求項1ないし4の何れか一項に記載のリモートアクセス制御方法。

【請求項6】 所定のネットワークに接続された複数のサーバへの、当該ネットワークの外部の端末からアクセスを制御するプログラムを、前記外部と前記所定のネットワークとの間に介在したサーバに実行させるリモートアクセス制御プログラムであって、

前記所定のネットワークに接続されたリモートアクセス制御サーバにおいて、

前記端末によるアクセスをなすユーザによる前記ネットワークへのログインのための認証情報を登録するステップと、

前記ユーザがアクセス可能な前記ネットワーク上のサーバのそれぞれに関する、当該ユーザの固有の認証情報を登録するステップと、

前記端末からの、前記ログインのための認証情報の受理に応答して、ユーザを認証するステップと、

認証されたユーザがアクセス可能なサーバに関するリストを生成して、当該リストを、前記端末に伝達するステップと、

前記端末からの、リストから選択された項目に基づき、前記ネットワーク上のアクセスすべきサーバを特定するステップと、

前記サーバに関する前記ユーザの固有の認証情報を取得して、当該サーバに対して、認証情報を伝達して、ユーザ認証および選択された項目に応答したコンテンツの伝達を求めるステップと、

前記サーバから、前記項目に応答したコンテンツを受理するステップと、

受理したコンテンツを、前記端末に伝達するステップとを、前記制御サーバに実行させることを特徴とするリモートアクセス制御プログラム。

【請求項7】 前記ユーザの固有の認証情報を登録するステップが、前記認証の種類を含み、

前記サーバに関する前記ユーザ固有の認証情報を、前記サーバに対して伝達するステップが、前記認証の種類にしたがった情報の伝達を行うように、前記制御サーバを動作させることを特徴とする請求項6に記載のリモートアクセス制御プログラム。

【請求項8】 前記サーバに関する前記ユーザ固有の認証情報を、前記サーバに対して伝達するステップが、ベーシック認証におけるユーザIDおよびパスワードを伝達するステップを含むように、前記制御サーバを動作させることを特徴とする請求項6または7に記載のリモートアクセス制御プログラム。

【請求項9】 さらに、前記受理したコンテンツにリンクが含まれる場合に、前記リンクを、前記リモートアクセスサーバを介した形態のものに変換するステップを、前記制御サーバに実行させることを特徴とする請求項6ないし8の何れか一項に記載のリモートアクセス制御プログラム。

【請求項10】 さらに、前記コンテンツにおけるフォ

ントサイズの変更、テーブルの列幅の調整を含むコンテンツ表示形態の調整、および／または、不要なタグの消去を含む、コンテンツを整形するステップを、前記制御サーバに実行させることを特徴とする請求項 6 ないし 9 の何れか一項に記載のリモートアクセス制御プログラム。

【発明の詳細な説明】

【0001】

【産業上の技術分野】本発明は、複数のサーバを有する一定のネットワーク、たとえば、社内イントラネットに

【0002】

【従来の技術】企業、地方公共団体などの組織内においては、サーバと多数の端末とを有線或いは無線にて接続して、情報を共有化するネットワークであるイントラネットが普及している。ここでは、ユーザは、端末から自己のアクセスが認められているサーバにアクセスして、必要な情報を引き出し、或いは、必要な情報を書き込むことができるようになっていく。

【0003】上記組織の構成員、たとえば、企業の社員などが、イントラネットの外部から、当該イントラネット上のサーバにアクセスして、必要な情報を取得する必要がある。これは、イントラネット上の一端を、所定の機器（たとえば、ゲートウェイ、ルータ）などを介して、インターネットに接続し、外部のコンピュータからインターネットを経て、イントラネット上のサーバ等にアクセス可能とすることにより実現される。特に、近年、パーソナルコンピュータによるアクセスではなく、インターネットに接続可能な携帯電話、PDAなどの携帯端末によるアクセス可能とすることが望まれる。

【0004】

【発明が解決しようとする課題】上記イントラネット上のサーバ等にアクセスする場合に、ユーザは、基本的には、自己が当該サーバにアクセスするためのパスワードなどの認証情報を、サーバに与える必要がある。たとえば、ベーシック認証においては、サーバごとに、自分のユーザIDおよびパスワードを入力し、サーバにおける認証の後、サーバとのアクセスが認められる。したがって、イントラネット上のサーバが複数存在する場合に、サーバごとの認証が必要となり、ユーザは、アクセスに至るまでに幾度となく認証情報の入力をする必要がある。また、サーバごとの認証では、各サーバ内のコンテンツ制御も煩雑となる。

【0005】本発明は、ユーザによる煩雑な入力なしに、一定のサーバにアクセス可能となるような手法を提供することを目的とする。

【0006】

【課題を解決するための手段】本発明の目的は、所定のネットワークに接続された複数のサーバに、当該ネットワークの外部の端末からアクセスするためのリモートア

クセス制御方法であって、前記所定のネットワークに接続されたリモートアクセス制御サーバにおいて、前記端末によるアクセスをなすユーザによる前記ネットワークへのログインのための認証情報を登録するステップと、前記ユーザがアクセス可能な前記ネットワーク上のサーバのそれぞれに関する、当該ユーザの固有の認証情報を登録するステップと、前記端末からの、前記ログインのための認証情報の受理に回答して、ユーザを認証するステップと、認証されたユーザがアクセス可能なサーバに関するリストを生成して、当該リストを、前記端末に伝達するステップと、前記端末からの、リストから選択された項目に基づき、前記ネットワーク上のアクセスすべきサーバを特定するステップと、前記サーバに関する前記ユーザの固有の認証情報を取得して、当該サーバに対して、認証情報を伝達して、ユーザ認証および選択された項目に回答したコンテンツの伝達を求めるステップと、前記サーバから、前記項目に回答したコンテンツを受理するステップと、受理したコンテンツを、前記端末に伝達するステップとを特徴とするリモートアクセス制御方法により達成される。

【0007】本発明によれば、制御サーバにおいて、所定のネットワーク、たとえば、社内イントラネットに接続された複数のサーバのそれぞれについて、ユーザがアクセス可能なサーバ、および、各サーバのユーザ固有の認証情報が登録されている。ユーザによる外部からの、所定のネットワークへのログイン要求に回答して、ユーザがアクセス可能な、当該ネットワーク上のサーバが見出され、これに関するリストがユーザの端末に提示される。ユーザのリスト中の項目の選択、すなわち、あるサーバへのアクセス要求に回答して、アクセス先のサーバに関するユーザ固有の認証情報が、登録された情報から取り出され、これを利用して、ユーザによる直接の認証の代理として、制御サーバによりネットワーク上のサーバに認証が依頼される。したがって、ユーザは、当該所定のネットワーク上のサーバにアクセスするたびに、認証のための入力、たとえば、ユーザIDやパスワードの入力の必要なく、自己がアクセスが認められている所望のサーバへのアクセスをなすことが可能となる。

【0008】本発明の好ましい実施態様においては、前記ユーザの固有の認証情報を登録するステップが、前記認証の種別を含み、前記サーバに関する前記ユーザ固有の認証情報を、前記サーバに対して伝達するステップが、前記認証の種別にしたがった情報の伝達を行うように構成されている。これにより、HTTPサーバ、メールサーバなど多種多様なサーバに対して、制御サーバが代理認証をなすことが可能となる。

【0009】より好ましい実施態様においては、サーバに関する前記ユーザ固有の認証情報を、前記サーバに対して伝達するステップが、ベーシック認証におけるユーザIDおよびパスワードを伝達するステップを含む。

【0010】別の好ましい実施態様においては、さらに、前記受理したコンテンツにリンクが含まれる場合に、前記リンクを、前記リモートアクセスサーバを介した形態のものに変換するステップを備えている。

【0011】さらに、前記コンテンツにおけるフォントサイズの変更、テーブルの列幅の調整を含むコンテンツ表示形態の調整、および／または、不要なタグの消去を含む、コンテンツを整形するステップを備えているのがより望ましい。携帯電話などディスプレイの小さな端末にコンテンツを伝達する場合に、これは特に有効である。

【0012】また、本発明の目的は、上記ステップを、制御サーバに実行させるためのリモートアクセス制御プログラムによっても達成される。

【0013】

【発明の実施の形態】以下、添付図面を参照して、本発明の実施の形態につき説明を加える。図1は、本発明の実施の形態にかかるデータ通信システムの概略を示す図である。図1に示すように、本実施の形態にかかるデータ通信システムは、インターネット12に、携帯電話やPDAなどの携帯端末14-1、・・・、14-nが接続されている。以下、単一の携帯端末を説明する際に、単に、「携帯端末14」と称する。

【0014】また、インターネット12には、携帯端末14がイントラネット24に接続されたサーバ26-1、・・・、26-mにアクセスする際に必要な処理を実行する制御システム16が接続されている。サーバに關しても、携帯端末14からのアクセスにかかるサーバを、単に、「サーバ26」と称する。

【0015】制御システム16は、携帯端末14との間でのインターネット12を介した通信の際に、データを、たとえば、SSLに基づき暗号化し、或いは、暗号化されたデータを復号化するリバースプロキシサーバ18と、HTMLのコンテンツを、携帯端末用の言語のコンテンツに翻訳するHTML変換サーバ(トランスコードサーバ)20と、イントラネット24へのアクセスの際に、後述する認証の代理などの処理を実行するリモートアクセス制御サーバ22とを有している。制御システム16のリモートアクセス制御サーバ22は、イントラネット24に接続されている。このイントラネット24には、種々のサーバ26-1、・・・、26-mが接続されている。

【0016】このシステムにおいては、インターネット12の側と、イントラネット24との間は、制御システム16にて隔てられている。たとえば、制御システム16には、ファイアウォールが形成され、オーソライズされていないユーザによる、インターネット12の側からのイントラネット24を介したアクセスが出来ないようにしている。たとえば、企業内のサーバ26-1、・・・、26-mを、イントラネット24にて接続した形

態を考える。企業内においては、社員つまりユーザが、クライアントマシンを操作してイントラネット24にログインして、当該イントラネット24上の、ユーザがアクセス可能なサーバにアクセスして、必要な情報を取得する。その一方、社外からのアクセスの際には、携帯端末14を利用して、制御システム16を介して、イントラネット24にログインして、イントラネット24上のサーバ26にアクセスすることになる。

【0017】次に、本実施の形態にかかるリモートアクセス制御サーバ22につき説明を加える。なお、リバースプロキシサーバ18およびHTML変換サーバ(トランスコードサーバ)20は、現段階で公知であるため、その機能の説明を省略する。図2は、本実施の形態にかかるリモートアクセス制御サーバ22の構成を示すブロックダイアグラムである。図2に示すように、リモートアクセス制御サーバ22は、インターネット12の側に接続され、当該インターネット12側との通信を制御するインターネット側通信I/F32を備えている。実際には、インターネット側通信I/F32は、HTML変換サーバ20に接続され、携帯端末14からの情報を受理し、或いは、携帯端末14に供給すべきデータ(コンテンツ)を伝達する。

【0018】また、リモートアクセス制御サーバ22は、インターネット12を介してアクセスしたユーザの、イントラネット24へのログインの際の認証を実行するユーザ認証部34と、上記イントラネット24へのログインの際に、ユーザを認証するための情報(ユーザID(UID)やパスワード(pwd))を記憶したユーザ認証情報データベース(DB)36と、ユーザによる初期的なアクセスに応答して、必要なメニューを生成する初期アクセスメニュー生成部38と、各ユーザがアクセス可能なサーバを示す情報が記憶されたユーザアクセス情報DB40と、イントラネットに接続された各サーバについての種々の情報が記憶されたイントラネットサーバ情報DB42と、携帯端末14に与えるためにコンテンツ中のURLを変更し、また、不要なタグ等を除去する処理を実行するHTML整形/表示部44と、初期的なアクセスの後、ユーザの携帯端末からのアクセス要求を受理して、必要な処理、特に、後述する代理認証の処理を実行するサーバアクセス要求受理部46と、イントラネット24と接続され、各サーバ26とのデータ通信を制御するイントラネット側通信I/F48と、イントラネット24を介して伝達されたコンテンツ等取得するデータ取得部50とを有している。

【0019】本実施の形態にかかるユーザ認証情報DB36、ユーザアクセス情報DB40、および、イントラネットサーバ情報DB42には、後述するような必要な情報が、予め登録されている。たとえば、ユーザ認証情報DB36へのユーザIDおよびパスワードの登録は、携帯端末14を用いて行っても良いし、イントラネット

24の側から（つまり、イントラネット24上の管理サーバなどから）行っても良い。また、ユーザアクセス情報DB40およびイントラネットサーバ情報DB42への登録は、イントラネット24の側から行うのが望ましい。

【0020】このように構成されたリモートアクセス制御サーバ22を介したデータ通信につき、以下に説明を加える。図3および図5は、携帯端末14、リモートアクセス制御サーバ22などにて実行される処理を示すフローチャートである。特に、図3は、携帯端末14からの初期的なアクセスの際に実行される処理を示している。図3において、携帯端末14とリモートアクセス制御サーバ22との間には、リバースプロキシサーバ18およびITM1変換サーバ20が介在しているが、これらサーバ18、20に関しては破線にて示し、その処理内容についての説明も省略している。

【0021】図3に示すように、携帯端末14からのログイン要求あり、携帯端末14からイントラネット24へのログイン用のユーザID（UID）およびパスワード（pwd）が伝達されると（ステップ301）、リモートアクセス制御サーバ22は、これを受理してユーザを認証する（ステップ302）。より詳細には、ユーザ認証部34が、ユーザ認証情報DB36に登録された、ユーザIDおよびそれに関連付けられたパスワードと、携帯端末14から伝達されたものとを照合する。

【0022】ユーザ認証が終了すると、初期アクセスメニュー生成部38が、ユーザアクセス情報DB40を参照して、ユーザがアクセス可能なサーバ等の情報を取得するとともに、イントラネットサーバ情報DB42をアクセスして、ユーザがアクセス可能なサーバに関する情報を取得して、所定のメニューを生成する（ステップ303）。図4（a）は、ユーザアクセス情報DB40中のデータ構造の例を示す図である。

【0023】図4（a）に示すように、ユーザアクセス情報DB40においては、ユーザごとにアクセス可能なサーバの名称、および、当該サーバの種別が記述されている（符号401、402参照）。たとえば、ユーザ「a」（ユーザID：usera）に関しては、デフォルト、httpサーバであるサーバ「A」（サーバ名：serverA）、メールサーバであるサーバ「B」（サーバ名：serverB）、httpサーバであるサーバ「D」（サーバ名：serverD）などにアクセス可能となっている（符号411、412参照）。

【0024】したがって、ユーザ「a」によるアクセスがあった場合には、初期アクセスメニュー生成部38は、ユーザアクセス情報DB40のうち、ユーザID「usera」に関するデータ（符号412）を参照して、ユーザ「a」がアクセス可能なサーバを特定する。次いで、イントラネットサーバ情報DB42のうち、当該ユーザがアクセス可能なサーバの各々に関するデータ

領域を参照する。

【0025】本実施の形態において、イントラネットサーバ情報DB42においては、各ユーザに共通にアクセス可能なサーバ情報であるデフォルト情報領域と、各サーバの情報領域とが設けられている。図4（b）は、デフォルト情報領域の例を示す図である。ここでは、メニューにリストされる際の優先順位（Priority）、アクセス先サーバ（Server）、アクセス先のコンテンツのタイトル（Title）、当該アクセス先のURL（URL）、携帯端末14にコンテンツを伝達する際に、元のコンテンツから消去すべきタグの情報（Delete TAG）、および、整形情報（Format）が含まれる。

【0026】携帯端末14に対して、送信するデータ量を小さくするのが望ましい。このため、文字嫉視の形態においては、IMGタグなどをコンテンツから削除できるようにしている。また、携帯端末14の表示装置の画面上にコンテンツを表示するため、フォントサイズを変更し、また、テーブルの列幅を調整する必要がある。このため、整形フォーマットには、上記フォントの変更や列幅の調整に関する記述が含まれ得る。さらに、コンテンツにはリンクが含まれる場合がある。本実施の形態において、外部からは、上記リンクに直接アクセスすることはできない。したがって、URLを変換するための情報が記述される場合もある。なお、図4（b）の例において、先頭行の「Is」はリストスタート用デリミタ、末尾の「Ie」はリストエンド用のデリミタである。図4（b）において、優先度は「0（最優先）」、サーバ名は「サーバA（serverA）」、タイトルは「サーバ「A」の基本コンテンツ」であることなどが示される。

【0027】また、図6は、各サーバの情報領域の例を示す図である。図6に示すように、情報領域600には、サーバ「A」（serverA）に関する情報領域（符号601参照）、サーバ「B」（serverB）に関する情報領域（符号602参照）、サーバ「C」（serverC）に関する情報領域（符号603参照）などが含まれる。

【0028】本実施の形態において、各情報領域には、当該サーバにアクセス可能なユーザごとに、以下に述べる項目を示す値が収容されている。サーバがウェブサーバである場合には、情報領域601には、アクセス可能なユーザ（たとえば、ユーザIDが「usera」）に関して、メニューにリストされる際の優先順位（Priority）、ベーシック認証をすべきか否かを示すフラグ（Basic Auth）、ベーシック認証時の保護領域（Realm）などが含まれる。サーバがメールサーバである場合には、情報領域602には、当該ユーザがメールサーバをアクセスする際の固有のパスワード（Password）などが含まれる。なお、情報領域

601、602、・・・には、サーバをアクセス可能なユーザごとに必要な項目の値が収容されるため、各ユーザに関する項目の値の最終行には、エンドオブユーザデリミタ(euc)が記述されている。

【0029】フラグ「BasicAuth」は、サーバによる認証がベーシック認証であるか否かを示している。また、保護領域「Realm」は、ベーシック認証によるパスワードにて保護される領域を示す。「Realm=test」であった場合には、「/test」以降の全ての領域、たとえば、

「http://serveraddress/test/index.html」

「http://serveraddress/test/subfolder/index.html」

などへのアクセスに際して、パスワードが必要であることを示している。初期アクセスメニュー生成部38は、アクセスにかかるユーザに関して、当該ユーザがアクセス可能なサーバの情報領域から、当該ユーザに関する項目の値を取得する。

【0030】次いで、アクセス可能なサーバ(より詳細には、サーバのURL)を示すタイトルからなるメニューを生成する。必要な場合には、フォントの変更、タグの削除などを含むメニューの整形などの処理を、HTML整形/表示部44が実行する。このようにして作られたメニュー画像は、HTML変換サーバ20およびリバースプロキシサーバ18を介して、インターネット12に送出され、アクセス元である携帯端末14に伝達される(ステップ305)。携帯端末14の表示装置の画面上には、アクセス可能なコンテンツのタイトルが列挙されたメニュー画像が表示される(ステップ306)。

【0031】次に、メニュー画像から所定のメニュー項目を選択した後に実行される処理につき、図5を参照して説明する。なお、図5において、携帯端末14とリモートアクセス制御サーバ22との間に介在するリバースプロキシサーバ18およびHTML変換サーバ20は省略している。

【0032】ユーザが携帯端末14のキーを操作して、所定のメニュー項目を選択すると、サーバアクセス要求受理部46が、このアクセス要求を受理する。ここで、図3のステップ305にて送信した情報には、セッションIDが含まれている。したがって、ステップ501におけるアクセス要求を受理したサーバアクセス要求受理部46は、セッションIDに基づいてユーザを特定する。次いで、サーバアクセス要求受理部46は、ユーザのアクセス要求にかかるサーバを特定して、イントラネットサーバ情報DB42から、当該サーバに関する情報領域中、アクセスしたユーザの固有パスワードを取得する(ステップ502、503)。

【0033】その後、ベーシック認証の代理処理(ステップ504)が実行される。より詳細には、ユーザがアクセス要求したURLに、イントラネット24を介して、アクセスして(ステップ505)、そこで、ユーザ

ID(UID)と、イントラネットサーバ情報DB42から取得した、当該サーバアクセスにかかるユーザ固有のパスワード(pwd)をアクセス先(たとえば、サーバ「A」)に伝達する(ステップ506)。アクセス先のサーバにおいては、当該ユーザIDおよび固有のパスワードに基づきユーザを認証し、正当なユーザである場合には、所定のコンテンツを、イントラネット24を介してリモートアクセス制御サーバ22に伝達する(ステップ508)。

10 【0034】リモートアクセス制御サーバ22は、取得したデータ(コンテンツ)が、HTMLでない場合(たとえば、アクセス先が、ウェブサーバではなく、メールサーバやデータベースサーバであった場合)には、取得したデータに基づくHTMLデータを生成する(ステップ509)。次いで、リモートアクセス制御サーバ22は、サーバに関する情報領域から不要タグや整形フォーマットに関する情報に基づき、データを整形する(ステップ510)。このようにして作られたデータ(コンテンツ)が、携帯端末14に伝達される(ステップ511)。このようにして、携帯端末14の表示装置の画面上には、ユーザが選択したメニュー項目にตอบสนองしたコンテンツが表示される(ステップ512)。

【0035】図7は、上記図3および図5にて示す処理により携帯端末14の表示装置の画面上に表示された画像の例を示す図である。ユーザによるログインの際には、携帯端末14の表示装置の画面上には、図7(a)に示す画像701が表示される。ユーザは、携帯端末14のキーを操作して、入力欄702、703に、それぞれ、ユーザIDおよびパスワードを記入する。このユーザIDおよびパスワードは、リモートアクセス制御サーバ22に登録されたものを利用すればよい。図7(b)は、これにตอบสนองして、ステップ305において伝達されたメニュー画像の例を示している。メニュー画像711から所定のメニュー項目(たとえば、「事務連絡掲示板(符号712参照)」)を選択すると、図5に示す処理が実行される。

【0036】再度説明すると、「事務連絡掲示板」へのアクセス要求(ステップ501)にตอบสนองして、当該「事務連絡掲示板」に関するサーバの情報領域から、アクセスしたユーザの固有パスワードが取り出され、イントラネット24を介して、上記サーバに対して、ユーザIDおよび取り出された固有パスワードが伝達される(ステップ506)。サーバにおいては、認証(ステップ507)の後、所定のコンテンツがリモートアクセス制御サーバ22に伝達される(ステップ508)。リモートアクセス制御サーバ22は、所定の処理(ステップ509、510)の後、コンテンツを携帯端末14に、インターネット12を介して伝達する(ステップ511)。図7(c)は、このようにして携帯端末14の表示装置の画面上に表示された画像721を示す。ここで、ユー

ザは、メニューから所望の項目を選択した後、当該メニュー項目に関するサーバのアクセスの際に、パスワードの入力などを行う必要がない。したがって、余分なキー入力なしに、自己がアクセスを認められている、イントラネット24上の所望のサーバにアクセスすることが可能である。

【0037】上記図5を参照した処理は、イントラネット24上のウェブサーバへのアクセスに関していたが、他のサーバ（たとえば、メールサーバやデータベースサーバ）に関連しても、代理認証の手法が異なるほかは略同様の手順にて実現される。

【0038】本実施の形態によれば、リモートアクセス制御サーバ22において、ユーザがアクセス可能なサーバ、および、各サーバをアクセスするためのそれぞれの固有パスワード（認証情報）を把握し、ユーザのアクセスにより、ユーザがアクセス可能なサーバのリストを含むメニュー画像を提示し、メニュー項目の選択にしたがって、選択されたメニュー項目に関するサーバをアクセスするためのユーザ固有のパスワードを利用して、認証を代理して実行する。したがって、ユーザは、サーバの

アクセスごとに、ユーザIDやパスワードの入力をする必要がなく、イントラネット24に接続された所望のサーバにアクセスして、所望のコンテンツを取得することが可能となる。

【0039】本発明は、以上の実施の形態に限定されることなく、特許請求の範囲に記載された発明の範囲内で、種々の変更が可能であり、それらも本発明の範囲内に包含されるものであることは言うまでもない。たとえば、前記実施の形態においては、携帯端末からのアクセスについて説明したが、これに限定されず、通常のパーソナルコンピュータからのアクセスについても本発明を適用できることは明らかである。

【0040】また、前記実施の形態においては、社内のイントラネット24へのアクセスに本発明を適用しているが、これに限定されず、地方公共団体、学校など任意の機関のイントラネットへのアクセスのために適用することが可能であることは言うまでもない。さらに、イントラネット24に限られず、インターネット12上であっても、一定のサーバ群が、リモートアクセス制御サーバ22を介してアクセスできるような構成に適用しても

良い。

【0041】また、本実施の形態においては、リモートアクセス制御サーバ22が、ベーシック認証、I MAP認証を、代理して実行しているが、リモートアクセス制御サーバ22が代理して実行できる認証種別は、上述したものに限定されるものではない。なお、本明細書にお

いて、一つの手段の機能が、二つ以上の物理的手段により実現されても、若しくは、二つ以上の手段の機能が、一つの物理的手段により実現されてもよい。

【0042】

【発明の効果】本発明によれば、ユーザによる煩雑な入力なしに、一定のサーバにアクセス可能となるような手法を提供することが可能となる。

【図面の簡単な説明】

【図1】 図1は、本発明の実施の形態にかかるデータ通信システムの概略を示す図である。

【図2】 図2は、本実施の形態にかかるリモートアクセス制御サーバの構成を示すブロックダイアグラムである。

【図3】 図3は、本実施の形態において、携帯端末、リモートアクセス制御サーバなどにて実行される処理を示すフローチャートである。

【図4】 図4は、本実施の形態にかかるユーザアクセス情報DB中のデータ構造、および、イントラネットサーバ情報DBのデフォルト情報領域の例を示す図である。

【図5】 図5は、本実施の形態において、携帯端末、リモートアクセス制御サーバなどにて実行される処理を示すフローチャートである。

【図6】 図6は、本実施の形態にかかるイントラネットサーバ情報DB中、各サーバの情報領域の例を示す図である。

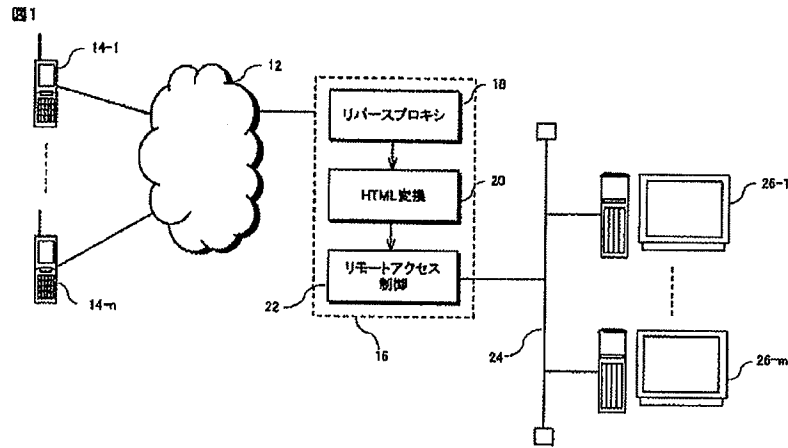
【図7】 図7は、本実施の形態において、携帯端末の表示装置の画面上に表示された画像の例を示す図である。

【符号の説明】

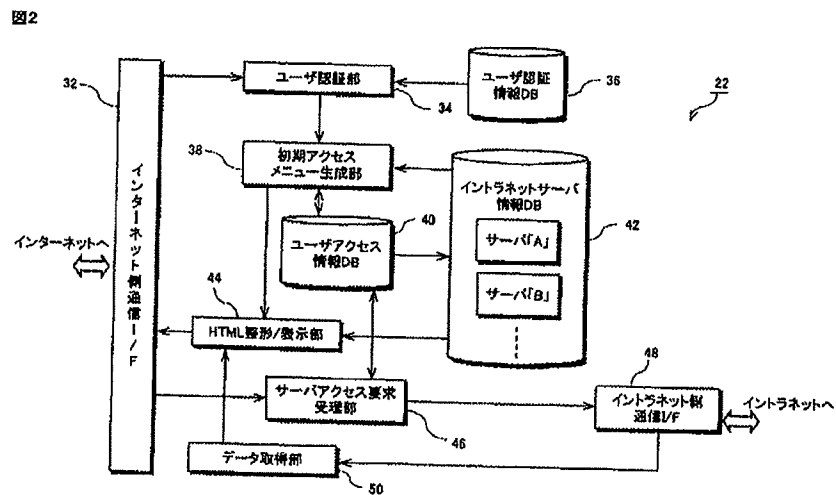
12	インターネット
14	携帯端末
16	制御システム
18	プロキシサーバ
20	HTML変換サーバ
22	リモートアクセス制御サーバ
24	イントラネット
26	サーバ
34	ユーザ認証部
36	ユーザ認証情報DB
38	初期アクセスメニュー生成部
40	ユーザアクセス情報DB
42	イントラネットサーバ情報DB
44	HTML整形／表示部
46	アクセス情報受理部
50	情報取得部



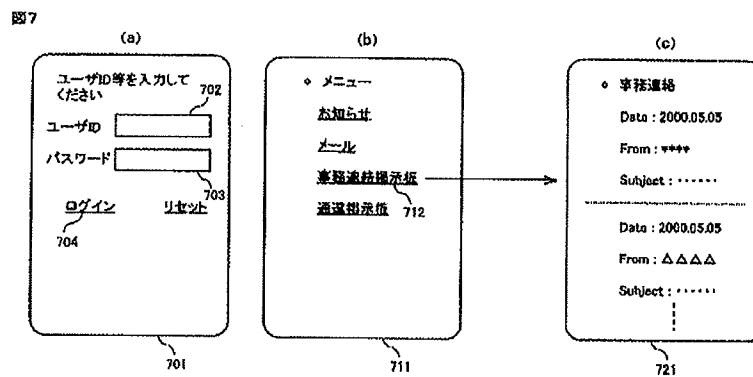
【図1】



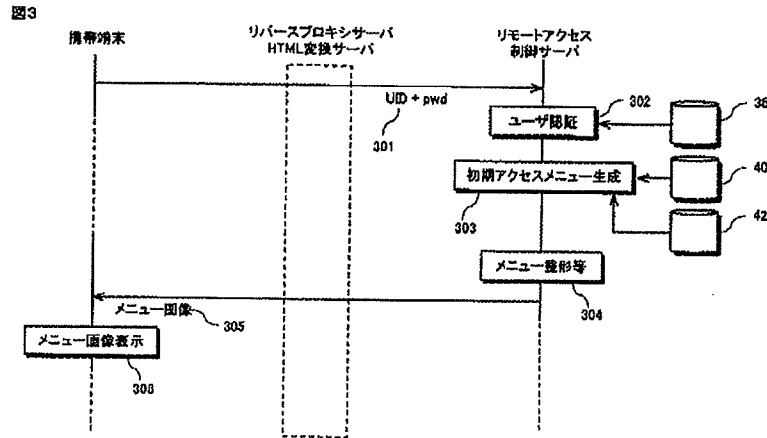
【図2】



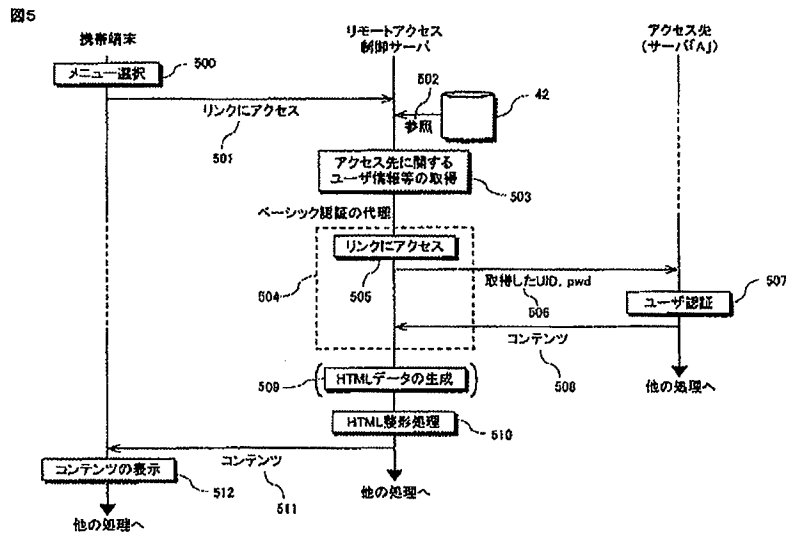
【図7】



【図3】

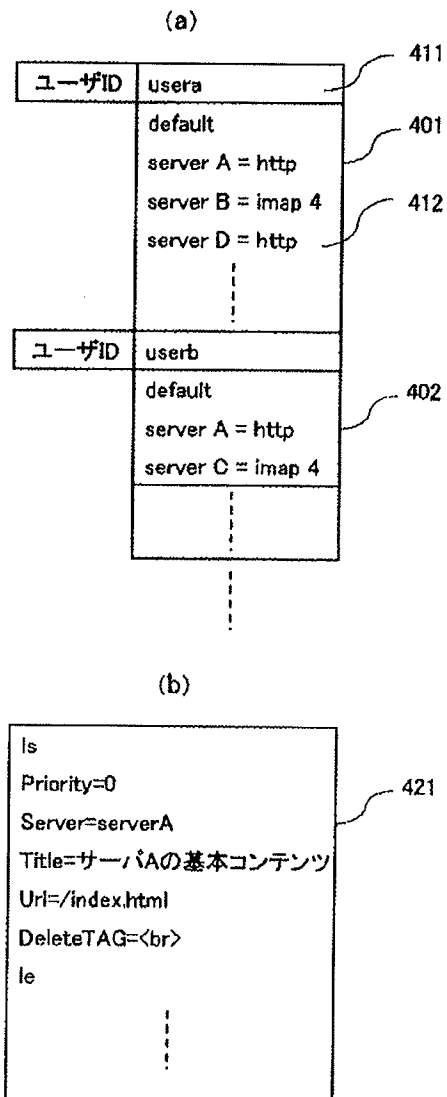


【図5】



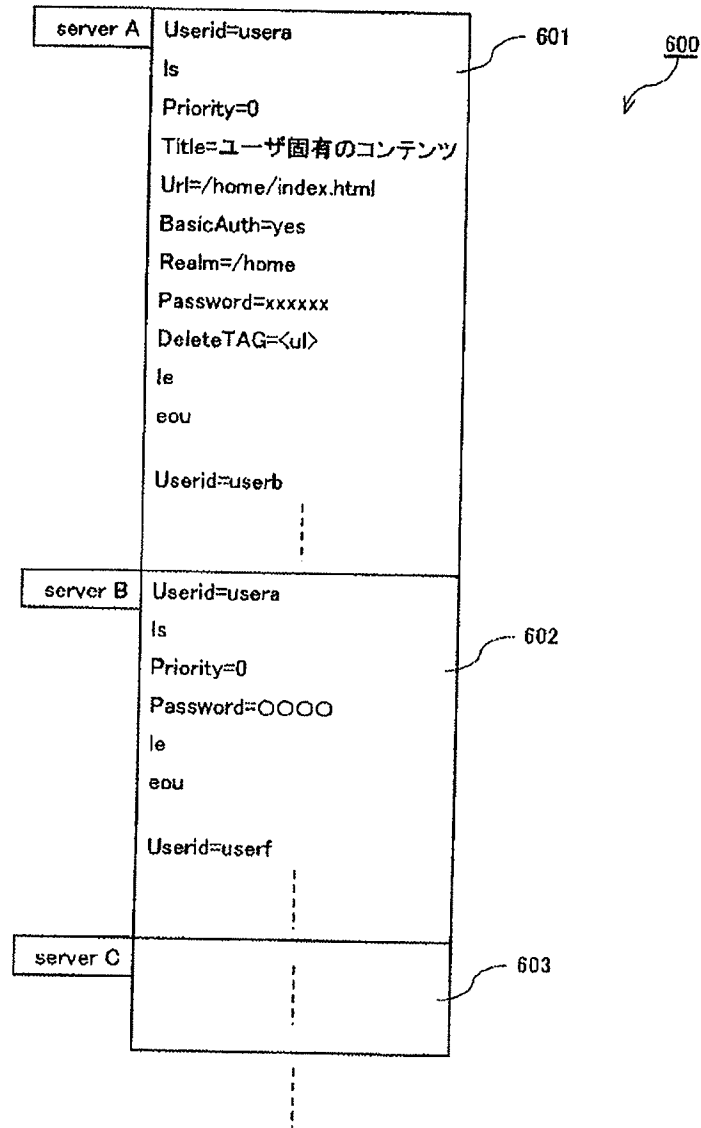
【図4】

図4



【図 6】

図 6



フロントページの続き

(51) Int. Cl.<sup>7</sup>  
G 0 6 F 13/00

識別記号  
5 1 0

F I  
G 0 6 F 13/00

キーワード(参考)  
5 1 0 A